

52/84

541

541 A

GOVERNMENT PUBLICATIONS REVIEW
GOVERNMENT PUBLICATIONS DEPARTMENT
UNIVERSITY OF NEVADA, RENO, NEVADA

1984 AND ALL THAT
OR MUST PRIVACY DIE? - AN AUSTRALIAN VIEWPOINT

June 1984

UNIVERSITY OF NEVADA, RENO, NEVADA

1984 AND ALL THAT
OR MUST PRIVACY DIE? -- AN AUSTRALIAN VIEWPOINT

Hon Justice MD Kirby CMG *

Chairman of the Australian Law Reform Commission 1975--

Judge of the Federal Court of Australia 1983--

WAS ORWELL RIGHT? DAME EDNA IS BORED

As it is 1984, somebody had better write to this Society about Orwell and his book of the year. Since Orwell wrote the book Ninety Eighty-four in 1948, the year 1984 has 'stood as a symbol of the way in which authoritarian attitudes and intrusive modern technology could undermine the freedom and individual privacy'.¹ In its major report on better privacy protection for Australia, the Australian Law Reform Commission, in December 1983, acknowledged that the book was a 'fantasy and parody' for Orwell. However, declared the report, 'enough reality already exists to constitute a warning to Australia that carefully designed legal responses are needed'.²

Over the past year or so, it has been difficult to pick up a newspaper in Australia without seeing mention of Orwell and his portrait of an oppressive, authoritarian state. Thus the publisher of the Privacy Journal in Washington, Robert Smith, recently

expressed his concern that the United States was threatened by the widespread imitations described in "1984", George Orwell's novel.

What we are allowing the computers to do to our society is quite upsetting. We seem to feel that computers have so much information about us that we shouldn't take any risks, that we should be compliant people. Public interest in privacy issues reached a peak from 1975 to 1977, when abuses of government power were uncovered in the congressional investigations of the Watergate scandals and activities of the CIA ... but with 1984, issues raised in George Orwell's novel seem to have revived a good deal of interest about where our society really is headed.³

A national opinion research survey of attitudes towards privacy in the United States disclosed that one in every three Americans believed that their society was 'very close to' or 'already like' the type of society described in George Orwell's book 1984 - a society in which 'virtually all personal privacy has been lost and the government knows almost everything that everyone was doing.'⁴ Almost one in ten Americans (9%) felt that their phone had been 'wire-tapped' at sometime. Public opinion polls on privacy conducted in Australia elicit similar results.⁵

Australians are prone to contra-suggestability. We are not alone in this. But we have developed intellectual cynicism to a fine art form. It will therefore be no surprise to learn that notable commentators on Orwell have spent much of 1984 questioning his relevance to the social predicaments we actually face. In fact, so strident has this questioning become that Orwell has been all but banished from the media of late. In a fine turn of contra-suggestability I have therefore decided to resurrect him. But what do the critics say?

Dame Dame Evelyn, a leading female member of the Australian Academy of Letters, reviewing a proposed film adaptation of *1984*, wrote that the book was "a masterpiece" and not as boring as 1984 had been made out to be. In 1984, James Orwell¹⁰ Antate historians will realize the stupid mistake. Whereas this blurb chose 'George' for his pseudonym, Dame Elin could not be bothered and dubbed 'George', 'James'.

In an essay, 'Rats! to 1984', Dr Michael Orange of the University of Sydney cautioned against getting carried away with Orwell:

Of course we need to be on guard against totalitarianisms of Right or Left. But it won't help us in the struggle to be politically vigilant if systems of government which we don't admire get inflated into fairytale monstrosities. We can't negotiate arms control agreements with demons who live in the forest, only with people. And those people have their own problems, have in particular their own fears. We need as much reasonableness as we can get, so at times it's important to say 'Rats!' to 1984, even if you know they'll get you in the end.⁷

In more studious vein, Dr AW Pryor of CSIRO and Macquarie University, at a symposium of the Australian & New Zealand Association for the Advancement of Science on '1984, Prediction and Reality' declared that Orwell was a novelist of our time. He reflected the depression of a world which fears that technology will turn us into slaves. But he cautioned that Orwell's frightened world was far worse than the reality.

Orwell's '1984' has a reputation of being the first of this new wave of disenchantment ... Orwell feared the last tyranny of all the tyrannies of the high minded reformer - Plato's 'republic' perfected by technology. But, all the same, '1984' is not a well-argued prediction of the future trends in society. We have

many problems this year but we do not have the same kind of totalitarian oppression envisaged by Orwell. Orwell's warning is not a prophecy, but a warning. The belief in the inevitable corruption of technology, as Huxley said, is not a warning, it is a prophecy. Now as ever, can be evil enough to be true.⁸

From across the Tasman come similar cautionary words against overstating the Orwellian warning. Radio New Zealand in its 'Sunday Supplement' described the book as 'one of the most overcrowded band-waggon of 1984'.⁹ Taking up this theme the New Zealand Minister of Justice and now Deputy Prime Minister Jim McLay said that most commentators had just got it wrong:

Nothing has been more boring than the hackneyed and overworked clichés that have obsessed newspaper, magazine, radio and television commentators desperate to give us their interpretation of George Orwell's story of a man who lives in a totalitarian state, under constant observation and subject to thought control by media manipulation ... The fact that Orwell originally intended to call his book '1949' is conveniently overlooked. So too is the fact that the novel was intended as a stinging criticism of Stalin's totalitarian Russia. So too is the fact that East Germany is the modern 1984 state that most closely resembles that in Orwell's book. These are the facts, but the cliché is far too good to be obscured by the facts. Self-appointed civil libertarians, journalists-with-nothing-better-to-do and bored — social — commentators have all issued their dark warnings of the imminent advent of 'Big Brother' ... [Orwell] warned of the dehumanizing potential of technology but did not appreciate, as one writer has since observed, that technology 'allow[s] us to see

unsuspecting people. In the wake of this disclosure, an atmosphere of fear has been
created in the use of telecommunications in the political arena.

Any sound that Winston made, above the level of a very low whisper, would be
picked up. Moreover, so long as he remained within the field in which the
metal plaque commanded, it could be seen as well as heard. There was, of
course, no way of knowing whether you were being watched at any given
moment. How often, or on what system the Thought Police plugged in on any
individual wire was guesswork. It was even conceivable that they watched
everybody all the time.

The Attorney-General of Australia, Senator Gareth Evans, has himself declared
that his telephone at Parliament House has been intercepted. Indeed, Senator Evans was
reported as believing that he had been the subject of a 'long-term Victorian phone-tap'.¹²

Federal Ministers have been warned to treat their parliamentary telephones as
'unsafe' after Senator Evans told the Australian Federal Cabinet on 16 April that he
believed his office telephones had been 'bugged'. Senator Evans asked ASIO to check his
telephones after 'irregularities' were discovered during a telephone conversation. The
irregularity apparently involved occurred when one of his staff members heard a tape
replay of a conversation just completed, repeated over the line.¹³

On the other side of politics Mr John Dowd, Shadow Attorney-General in New
South Wales, was reported as having fears that his Parliamentary Office was being
'bugged'. 'I have a lot of information here', he said, 'that other people would dearly love to
get their hands on'.¹⁴

that were not checked. The Prime Minister of Australia, Mr Hawke, has expressed his fear that even the police might be tempted to tap phones. He expressed a view that anyone who would be tempted to do so would be a 'bad apple' who should be 'tapped'.¹⁵ Later, speaking to a house which included Mr Hawke and I knew that I have had conversations on phones that if they were made openly would be capable of misrepresentation. I have certainly said things on the telephone of which I would be ashamed -- and so has every single person. In a timely way, Mr Hawke warned of the danger of the unrestricted use and publication of illegally obtained telephone conversations.¹⁶

Justice Hope, the Royal Commissioner investigating the security and intelligence agencies, has heard allegations that the Defence Signals Directorate has illegally tapped telephone calls in Australia, allegedly because of the fear that the Attorney-General would not issue a warrant as he is empowered to do by law.¹⁷

In late May 1984 it was reported that the telephone of Justice Slattery, the Special Commissioner investigating a New South Wales Minister Rex Jackson, accused of corrupt practices, had been checked by Federal Police for bugging devices.¹⁸ It will be recalled that Justice Slattery was himself in possession of transcripts of legal telephonic interceptions which had been authorised in respect of Mr Jackson's telephone. Special Federal legislation had been enacted authorising the release of these intercepts to the Special Commission of Inquiry.

Notwithstanding all the fears and denunciations, it is now reported that Federal Government agencies in Australia, in a bid to stop the spread of illegal SP bookmaking, are considering actually widening Federal phone tapping legislation. According to reports, the proposed changes are aimed at allowing police to use Telecom's 'scrap machines' or call record printers (CRP) to monitor the telephones of suspected SP operators. The

machine permits a record to be taken of all telephone numbers dialed and the duration of the call. In some ways this record would be more damaging than a direct interception of the conversation because it is not that a connection without offering the possibility of conclusive evidence as to a total innocence.¹⁹

Whilst the telecommunications interceptions by State Police in Australia may have been illegal (and are now to be further prohibited and controlled by State legislation²⁰) the move to the computerisation of police data in Australia is well advanced. Instead of a radio call to an overloaded communications room for routine information, computer terminals linked to integrated criminal intelligence systems will soon be able to provide instantaneous data on virtually every citizen -- from the cradle to the grave.²¹

There are many other developments that give rise to concern for our civil liberties in the age of informatics. The growing use of credit cards in the cashless society will provide a 'credit trail' that constitutes a vivid daily biography of an increasing number of citizens. The all-seeing television screen predicted by Orwell may not be needed if every transaction of life can be recorded and centrally maintained, analysed and presented to authority. Everywhere you go. Every book you buy. This is not a far-distant nightmare. It is a technology that is virtually with us already. As a society, we must ask whether we accept the inevitable erosions of individual privacy and anonymity. Or whether we should lay down rules that we have the courage to enforce, even when it seems hard to do so. Of course, it is hard to exclude the future use of sensational telephone conversations illegally obtained. Yet, rights matter most when important freedoms are at risk.²² It is tempting to publish and be damned. To do so can always be cloaked in a self-righteous appeal to the freedom of the press. But there is a competing

...the erosion of privacy by interception of telephonic conversations and a free society. ...the erosion of privacy by interception of telephonic conversations and a free society. ...the erosion of privacy by interception of telephonic conversations and a free society.

In the early days of the Australian Law Reform Commission the dangers, including the chilling effect of widespread telephonic interception were called to notice. Relying on the reported figure of 107 legal Australian phone taps in 1973, the Australian Law Reform Commission said in a 1975 report:

If American figures as to the ratio of persons and conversations overheard to wire taps installed are any kind of guide, it may indeed have been the case that a 107 wire taps to the year ending March 1973 resulted in the overhearing of as many as 12,000 different people engaged in as many as 63,000 conversations.²³

Prophetically, the Commission in 1975 called attention to the illegal use of telephonic interception by State police forces. It recorded that the former Prime Minister, Mr Menzies, had written to the then Premier of New South Wales to ask that New South Wales Police have their attention drawn to Federal legislation on telephonic interception and be requested to avoid future contraventions of rules and limitations on police phone taps.²⁴ A similar letter was written by Federal Attorney-General Greenwood to the Queensland Attorney-General in 1972 protesting at the illegal interception of telephone conversations by Queensland police.²⁵ Have we now become so inured to the erosion of privacy by interception? Is the finding of the occasional miscreant in this way worth paying the price of the virtually total destruction of the community's long held confidence in the privacy of its telephonic system? Given the United States figures, is it only guilty people who have to worry about being caught up in the web of interception? Or will not very large numbers of perfectly innocent good citizens be caught up in an expanding net of official surveillance? Are we to take our laws on wire taps seriously or must we watch helpless at the death of privacy in Australia?

These are legitimate questions the Australian community should be asking itself in 1984. They, and other questions, were raised in the Law Reform Commission's report on privacy protection.

THE REPORT ON BETTER PRIVACY PROTECTION

Beyond Computers. The privacy report of the Australian Law Reform Commission identifies the chief threats to privacy in modern Australia. They are:

- . new surveillance technology, telephone taps, listening devices and hidden cameras; but also
- . growing official powers of intrusion;
- . new invasive business practices;
- . new information technology, computers linked by telecommunications.

The central recommendation of the Law Reform Commission's report on privacy was the proposal to establish a 'privacy watchdog'. But there were many other proposals:

- . enlargement of the Federal Human Rights Commission to assume new and special responsibilities for privacy protection as contemplated by the International Covenant on Civil and Political Rights;
- . provision of statutory guiding rules for the evaluation of complaints about privacy invasion;
- . specific limitations on specially invasive body cavity searches by Federal officials;
- . new Federal legislation to control secret surveillance by listening and optical devices;
- . extension of present legislation to tighten up rules against telephone tapping and intrusions into the privacy of the mail.

in developing its proposals, the Australian Law Reform Commission dated attention to

- . expand the suggested model so that it will apply in the States, whose laws presently govern the great part of privacy regulation in Australia;
- . expand Federal regulation by utilising relevant Federal heads of constitutional power such as those which permit the Commonwealth to make laws governing the States on banking, insurance, corporations and external affairs; and
- . develop Australia's laws in the context of international developments in information technology and fast-expanding international rules governing informatics (the linkage of computers and telecommunications).

The Australian Law Reform Commission's report specifically rejects the creation of a vague and general civil remedy of privacy protection. It also rejects confining privacy protection to computerised personal information systems. It acknowledges the general desirability of facilitating the free flow of information and that this can sometimes lead to a clash with privacy interests. It suggests that privacy laws should be developed to supplement present Australian laws which already partly protect this interest. But it urges early attention to its recommendations:

Unless legislative and other actions are taken for the better protection of privacy, this important attribute of freedom may be irretrievably lost.²⁶

Information privacy. The Commission's report declared that one of the most important sources of danger for privacy of the Australian today arose from the remarkable technology of informatics. I use that word, although I know that it has not yet gained universal currency. To refer to computers is now inadequate, for computers have now been married to telecommunications. To refer to 'computations' as one

French Minister did, is unacceptable because it is irredeemably ugly. Information technology' is a mouthful. In any case, it will remind most ordinary citizens of propaganda machines or conjure up images of a compositor or a printing press. I now make up for the 'informatics'. It is a simply single word increasingly accepted in the OECD. We should get used to it in Australia. Informatics -- the word and the phenomenon -- is here to stay.

The features of informatics mentioned in the privacy report as factors that increase the risk to individual privacy include:

- . the vastly increased amounts of personal information that can now be stored virtually indefinitely;
- . the enormous increase in the speed and ease of retrieval of such information now technologically possible;
- . the substantial reduction in the cost of handling, storing and retrieving such information which makes it tempting to keep it just in case it may prove useful;
- . the constant establishment of cross-linkages between information systems permitting searching and matching of data supplied for numerous purposes;
- . the capability of building up a composite profile, one which is no more accurate than the many sources of the data and which may, in aggregate, distort and misrepresent the data subject;
- . the creation of an entirely new profession, 'computerists', or 'informaticists', largely unrestrained by law and unevenly restrained by established professional codes of conduct;
- . the greater ease of accessibility to personal data, despite codes and occasional encryption, when the technologist is really determined;
- . the tendency to centralise control of personal data;
- . the rapid advance of international telecommunications, diminishing the power of domestic governments and lawmakers to enforce local perceptions of fairness and privacy.

The Australian Law Reform Commission's recommendations address these problems and propose creation of a series of principles by which complaints for access to information can be evaluated and dealt with by the Privacy Commissioner. In addition, the proposals adopt the so-called 'golden rule' of privacy protection found in legislation in Europe and North America. This is the right of the data subject normally to have access to personal data about him- or herself. It is a right of access which must succumb to exceptions in certain circumstances. The approach taken is:

- . there should be a right, enforceable under Federal law, by which the individual will be entitled, unless excluded by law, to have access to both public and private sector records of personal information held about him- or herself;
- . where it is found that this information is incorrect, incomplete, out of date or misleading, procedures for correction of the record or addition of appropriate notations should be available;
- . in addition to this enforceable right, rules are proposed to govern the use, disclosure and security of personal information. Suspected breach of these rules can be investigated by the Privacy Commissioner and can be the subject of ombudsman-like remedies.

The Law Reform Commission's report expands and clarifies the right of access, already found in the Federal, Victorian and proposed New South Wales freedom of information legislation. It clarifies the right and pushes it for the first time into the private sector in the context of Federal regulation of the Australian Capital Territory. The report makes it plain that the Law Reform Commission was limited by the terms of its reference and the Australian Constitution from expanding this central privacy right of access to a much wider field in the private sector. It leaves any such expansion of privacy protection as tasks for the future.

privacy principles. It also leaves for the future the question of whether any of the other information privacy principles -- largely derived from the OECD Guidelines on Trans-Border Data Flows and the Protection of Privacy -- could be developed into enforceable rules -- ie rules which, like the right of access, can be directly enforced by the data subject. For this reason, it is perhaps useful to state the 'information privacy principles'. They are set out in a schedule annexed to the draft Privacy Bill which is in turn attached to the Law Reform Commission's report. Under clause 7 of that Bill it is declared that:

where a person does an act or acts in accordance with a practice that is contrary to or inconsistent with anything set out in the schedule, the act or practice shall be taken to be an interference with the privacy of a person.²⁷

These are the information privacy principles proposed by the Australian Law Reform Commission:

Collection of Personal Information

1. Personal information should not be collected by unfair or unlawful means, nor should it be collected unnecessarily.
2. A person who collects personal information should take reasonable steps to ensure that, before he collects it or, if that is not practicable, as soon as practicable after he collects it, the person to whom the information relates (the 'record-subject') is told --
 - (a) the purpose for which the information is being collected (the 'purpose of collection'), unless that purpose is obvious;
 - (b) if the collection of the information is authorised or required by or under law -- that the collection of the information is so authorised or required; and
 - (c) in general terms, of his usual practices with respect to disclosure of personal information of the kind collected.

2. A person should ensure that collection, use and disclosure of personal information is limited to the purpose of collection and is not disclosed to third parties unless it is exclusively personal.

Storage of Personal Information

4. A person should take such steps as are, in the circumstances, reasonable to ensure that personal information in his possession or under his control is securely stored and is not misused.

Access to Records of Personal Information

5. Where a person has in his possession or under his control records of personal information, the record-subject should be entitled to have access to those records.

Correction of Personal Information

6. A person who has in his possession or under his control records of personal information about another person should correct it so far as it is inaccurate or, having regard to the purpose of collection or to a purpose that is incidental to or connected with that purpose, misleading, out-of-date, incomplete or irrelevant.

Use of Personal Information

7. Personal information should not be used except for a purpose to which it is relevant.
8. Personal information should not be used for a purpose that is not the purpose of collection or a purpose incidental to or connected with that purpose unless —

- (c) the record-subject has consented to the use;
 - (d) the person using the information believes on reasonable grounds that the use is necessary to prevent or lessen a serious and imminent threat to the life or health of record-subject or of some other person; or
 - (e) the use is required by or under law.
9. A person who uses personal information should take reasonable steps to ensure that, having regard to the purpose for which the information is being used, the information is accurate, complete and up to date.

Disclosure of Personal Information

10. A person should not disclose personal information to another person unless --
- (a) the record-subject has consented to the disclosure;
 - (b) the person disclosing the information believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of record-subject or of some other person; or
 - (c) the disclosure is required by or under law.

The Australian report does not confine itself in its application to personal information to informatics personal data. In other words, it is neutral as to the technology by which the personal information is kept. This conclusion was reached partly as a result of the Commission's terms of reference, partly from considerations of the Australian Constitution but partly also from reflection upon the dangers that can just as readily arise to personal privacy from an old-fashioned paper notebook or a manilla folder in the bottom drawer. Strictly speaking, then, this is not a data protection and data security statute, such as has been enacted in many European countries and proposed in England. The Australian Law Reform Commission's proposal addresses generically the problem of privacy protection. It is neutral as to the medium used for the abuse of privacy. It is candid in its

... of future legislation specific to informatics may be needed. The report
... and ... on ... a step on the long path of
... values that are challenged by the new information technology.

CONCLUSIONS : WOODY ALLEN AND OUR CHOICE

This essay may seem depressing from the Antipodes. Yet everybody knows that the good news of technology brings with it the bad news of the need for uncomfortable social adjustment. There are many other social problems that come in the train of informatics. They will require attention by Australian society. They are identified in the Australian Law Reform Commission's privacy report. They include the impact of structural unemployment, the growth of vulnerability of the wired society, the growing potential for computer crime, the relative loss of cultural, political and economic sovereignty, the loss of jurisdictional legal autonomy and so on. There are special problems in Australia in tackling these issues in a coherent and well thought out way. The Australian Federal Constitution, which long preceded the development of computers, does not encourage a national approach. In recent weeks, the Queensland Parliament has proceeded with its own Privacy Committee Bill.²⁸ A serious question will be raised as to whether, with such a pervasive and universal technology, Australia can afford the luxury of disparate approaches to regulation in its several State jurisdictions.

Woody Allen in a recent graduation address in the United States declared:

More than any other time in history, mankind faces a crossroads. One path leads to despair and utter hopelessness. The other, to total extinction. Let us pray we have the wisdom to choose correctly.²⁷

If we escape the nuclear holocaust, must we really contemplate the utter insignificance of the Orwellian nightmare? Is it beyond our wit and will in the age of the microchip, the satellite, laser and other information technology to preserve at least the central features of individual freedom and personal privacy, the rule of law and optimistic, reforming institutions? I trust that Woody Allen for once got it wrong that Australian society, at least, will have the wisdom to perceive its predicament and in an age of science and technology, to preserve and defend its enduring human values.

FOOTNOTES

- * Personal views only.
- 1. Australian Law Reform Commission, Privacy, 1983 (ALRC 22) Vol 1, xli.
- 2. ibid.
- 3. RE Smith, 'Computers Cause Privacy Worries', Sydney Morning Herald 16 April 1984, 3.
- 4. L Harris and Associates, The Dimensions of Privacy: A National Opinion Research Survey of Attitudes Towards Privacy, 1979, 5.
- 5. ALRC 22, 4.
- 6. Quoted Weekend Australian, 11 February 1984, 1.
- 7. M Orange, 'Rats!', to 1984', Airways Magazine, January 1984. 13.

8. A.W. Pryor, Science, Technology and the Future, ANZAS Symposium, 1984 'Prediction of Reality', 28 March 1984, pp. 1, 2.
9. Cited by J.L. Wile, address, New Zealand, February 1984, mimeo, 11.
10. ibid.
11. B Stannard, 'Atmosphere of Fear in Wake of the Tapes', in The Bulletin 10 April 1984, 24.
12. ibid.
13. GJ Evans, Australian, 19 April 1984, 1.
14. Cited The Bulletin, 10 April 1984, 25.
15. The Age, 4 March 1984, 5.
16. The Age, 17 March 1984, 7.
17. Sydney Morning Herald, 4 April 1984, 11.
18. Canberra Times, 29 May 1984, 1.
19. Reported Sydney Morning Herald, 13 March 1984.
20. See announcement of NSW legislation in Weekend Australian, 19-20 May 1984, 10.
21. M Brown, 'A Computerised Police Force', Sydney Morning Herald, 5 March 1984, 6.

21. Offit Harding reported Canberra Times, 23 March 1984, 8.
22. Australian Law Reform Commission, Criminal Investigation (ALRC 22, 1982).
23. *id.*
24. Queensland, Parliamentary Debates (Legislative Assembly), 28 March 1984, 2158.
25. ALRC 22, Vol 1, xlv.
26. *ibid*, Vol 2, 216. See also, 255.
27. Queensland, Parliamentary Debates (Legislative Assembly) 28 March 1984, 2185.
28. Woody Allen cited B Jones, 'The Role and Problem of the Principal', address to the Headmasters' Conference of the Independent Schools of Australia, 1 July 1983, mimeo, 1.